

# Report Tecnico: Network Traffic Analysis

## Forensic Analysis of TCP Port Scanning Activity

Studente: Josh Van Edward D Abanico

Data: 6 febbraio 2026

No.	Time	Source	Destination	Protocol	Length	Info
63	0.2374431	192.168.200.150	192.168.200.150	TCP	60	63 53500 → 80 [RST] Seq=1 Win=0 Len=0
64	0.2374431	192.168.200.150	192.168.200.150	TCP	60	64 53500 → 80 [ACK] Seq=1 Win=0 Len=0
65	0.2374431	192.168.200.150	192.168.200.150	TCP	60	65 53500 → 80 [ACK] Seq=1 Win=0 Len=0
66	0.2374431	192.168.200.150	192.168.200.150	TCP	60	66 53500 → 80 [ACK] Seq=1 Win=0 Len=0
67	0.2374431	192.168.200.150	192.168.200.150	TCP	60	67 53500 → 80 [ACK] Seq=1 Win=0 Len=0
68	0.2374431	192.168.200.150	192.168.200.150	TCP	60	68 53500 → 80 [ACK] Seq=1 Win=0 Len=0
69	0.2374431	192.168.200.150	192.168.200.150	TCP	60	69 53500 → 80 [ACK] Seq=1 Win=0 Len=0
70	0.2374431	192.168.200.150	192.168.200.150	TCP	60	70 53500 → 80 [ACK] Seq=1 Win=0 Len=0
71	0.2374431	192.168.200.150	192.168.200.150	TCP	60	71 53500 → 80 [ACK] Seq=1 Win=0 Len=0
72	0.2374431	192.168.200.150	192.168.200.150	TCP	60	72 53500 → 80 [ACK] Seq=1 Win=0 Len=0
73	0.2374431	192.168.200.150	192.168.200.150	TCP	60	73 53500 → 80 [ACK] Seq=1 Win=0 Len=0
74	0.2374431	192.168.200.150	192.168.200.150	TCP	60	74 53500 → 80 [ACK] Seq=1 Win=0 Len=0
75	0.2374431	192.168.200.150	192.168.200.150	TCP	60	75 53500 → 80 [ACK] Seq=1 Win=0 Len=0
76	0.2374431	192.168.200.150	192.168.200.150	TCP	60	76 53500 → 80 [ACK] Seq=1 Win=0 Len=0
77	0.2374431	192.168.200.150	192.168.200.150	TCP	60	77 53500 → 80 [ACK] Seq=1 Win=0 Len=0
78	0.2374431	192.168.200.150	192.168.200.150	TCP	60	78 53500 → 80 [ACK] Seq=1 Win=0 Len=0
79	0.2374431	192.168.200.150	192.168.200.150	TCP	60	79 53500 → 80 [ACK] Seq=1 Win=0 Len=0
80	0.2374431	192.168.200.150	192.168.200.150	TCP	60	80 53500 → 80 [ACK] Seq=1 Win=0 Len=0
81	0.2374431	192.168.200.150	192.168.200.150	TCP	60	81 53500 → 80 [ACK] Seq=1 Win=0 Len=0
82	0.2374431	192.168.200.150	192.168.200.150	TCP	60	82 53500 → 80 [ACK] Seq=1 Win=0 Len=0
83	0.2374431	192.168.200.150	192.168.200.150	TCP	60	83 53500 → 80 [ACK] Seq=1 Win=0 Len=0
84	0.2374431	192.168.200.150	192.168.200.150	TCP	60	84 53500 → 80 [ACK] Seq=1 Win=0 Len=0
85	0.2374431	192.168.200.150	192.168.200.150	TCP	60	85 53500 → 80 [ACK] Seq=1 Win=0 Len=0
86	0.2374431	192.168.200.150	192.168.200.150	TCP	60	86 53500 → 80 [ACK] Seq=1 Win=0 Len=0
87	0.2374431	192.168.200.150	192.168.200.150	TCP	60	87 53500 → 80 [ACK] Seq=1 Win=0 Len=0
88	0.2374431	192.168.200.150	192.168.200.150	TCP	60	88 53500 → 80 [ACK] Seq=1 Win=0 Len=0
89	0.2374431	192.168.200.150	192.168.200.150	TCP	60	89 53500 → 80 [ACK] Seq=1 Win=0 Len=0
90	0.2374431	192.168.200.150	192.168.200.150	TCP	60	90 53500 → 80 [ACK] Seq=1 Win=0 Len=0
91	0.2374431	192.168.200.150	192.168.200.150	TCP	60	91 53500 → 80 [ACK] Seq=1 Win=0 Len=0
92	0.2374431	192.168.200.150	192.168.200.150	TCP	60	92 53500 → 80 [ACK] Seq=1 Win=0 Len=0
93	0.2374431	192.168.200.150	192.168.200.150	TCP	60	93 53500 → 80 [ACK] Seq=1 Win=0 Len=0
94	0.2374431	192.168.200.150	192.168.200.150	TCP	60	94 53500 → 80 [ACK] Seq=1 Win=0 Len=0
95	0.2374431	192.168.200.150	192.168.200.150	TCP	60	95 53500 → 80 [ACK] Seq=1 Win=0 Len=0
96	0.2374431	192.168.200.150	192.168.200.150	TCP	60	96 53500 → 80 [ACK] Seq=1 Win=0 Len=0
97	0.2374431	192.168.200.150	192.168.200.150	TCP	60	97 53500 → 80 [ACK] Seq=1 Win=0 Len=0
98	0.2374431	192.168.200.150	192.168.200.150	TCP	60	98 53500 → 80 [ACK] Seq=1 Win=0 Len=0
99	0.2374431	192.168.200.150	192.168.200.150	TCP	60	99 53500 → 80 [ACK] Seq=1 Win=0 Len=0
100	0.2374431	192.168.200.150	192.168.200.150	TCP	60	100 53500 → 80 [ACK] Seq=1 Win=0 Len=0

Oggetto: Analisi Forense - Port Scanning Detection  
Tool Utilizzato: Wireshark

# Indice

<b>1</b>	<b>Introduzione e Scenario Operativo</b>	<b>2</b>
1.1	Obiettivi dell'Analisi . . . . .	2
1.2	Topologia della Rete Ricostruita . . . . .	2
<b>2</b>	<b>Fase 1: Analisi Cronologica dell'Attacco</b>	<b>2</b>
2.1	Annuncio Spontaneo della Vittima . . . . .	2
2.2	Verifica Attività (TCP Ping) . . . . .	2
2.3	Network Discovery (ARP) . . . . .	3
2.4	Attacco alle "Top Ports" (Initial Burst) . . . . .	3
2.5	Enumerazione Infrastruttura e Mail (Second Wave) . . . . .	4
2.6	Chiusura Sessioni e Noise Scanning . . . . .	5
2.7	Rilevamento Servizi Legacy Critici (Porta 512) . . . . .	5
2.8	Conferma Vulnerabilità R-Services (Porta 514) . . . . .	6
2.9	Identificazione R-Login (Porta 513) . . . . .	6
<b>3</b>	<b>Fase 2: Approfondimento Tecnico (Stealth vs Connect)</b>	<b>8</b>
3.1	Differenze Teoriche: TCP Connect vs SYN Stealth . . . . .	8
3.2	Analisi Forense . . . . .	8
3.3	Deduzione Investigativa . . . . .	8
<b>4</b>	<b>Fase 3: Risultati dell'Enumerazione</b>	<b>10</b>
4.1	Criticità Massima: Suite "R-Services" (Legacy) . . . . .	10
4.2	File Sharing e Infrastruttura . . . . .	10
4.3	Accesso Remoto e Web . . . . .	10
<b>5</b>	<b>Conclusioni</b>	<b>11</b>

# 1 Introduzione e Scenario Operativo

## 1.1 Obiettivi dell'Analisi

Il presente documento riporta l'analisi tecnica di una cattura di traffico di rete (PCAP). L'obiettivo primario è caratterizzare la tipologia di traffico anomalo rilevato tra due host della rete locale, identificare le tecniche di ricognizione utilizzate dall'attaccante e mappare la superficie di attacco esposta dalla vittima.

## 1.2 Topologia della Rete Ricostruita

Dall'analisi dei pacchetti ARP (Address Resolution Protocol) e del traffico TCP, è stata definita la seguente topologia:

- **Attaccante (Scanner):** 192.168.200.100
- **Vittima (Target):** 192.168.200.150
- **Asset Inventory:** Il target è identificato come una macchina virtuale "Metasploitable 2", progettata intenzionalmente con vulnerabilità per scopi di testing (banner rilevato nel pacchetto n. 1).

# 2 Fase 1: Analisi Cronologica dell'Attacco

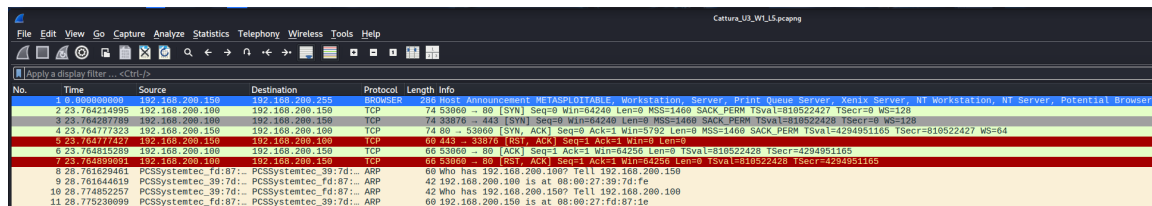
## 2.1 Annuncio Spontaneo della Vittima

Al pacchetto n. 1 (Time 0.000), la macchina vittima invia un messaggio broadcast **NetBIOS Host Announcement**, rivelando spontaneamente la propria presenza e il proprio nome host ("METASPLOITABLE") all'intera rete, senza alcuna sollecitazione esterna.

## 2.2 Verifica Attività (TCP Ping)

Circa 5 secondi prima della scansione principale (pacchetti 2-7), l'attaccante esegue un controllo di disponibilità ("Host Discovery") per verificare se il target è attivo. Vengono inviati pacchetti **SYN** mirati verso le porte standard **80 (HTTP)** e **443 (HTTPS)**.

- La ricezione di un [SYN, ACK] dalla porta 80 (pacchetto 4) conferma all'attaccante che l'host è acceso e raggiungibile.
- L'attaccante chiude immediatamente la connessione preliminare con un RST (pacchetto 7), avendo ottenuto la conferma necessaria per procedere con l'attacco massivo.

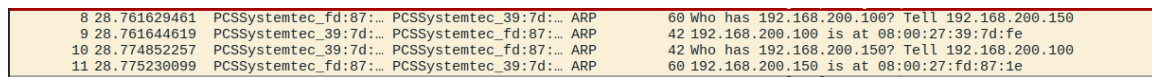


No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.150	192.168.200.100	UDP	44	Host Announcement (who has 192.168.200.150?)
3	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
4	23.764217788	192.168.200.100	192.168.200.150	TCP	74	53060 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
5	23.764217788	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
6	23.764217788	192.168.200.150	192.168.200.100	TCP	68	443 → 53060 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	23.764217788	192.168.200.100	192.168.200.150	TCP	68	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230699	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

Figura 1: Pre-Attacco: Host Announcement spontaneo e TCP Ping di verifica (Porte 80/443).

## 2.3 Network Discovery (ARP)

L'attività ostile inizia con una fase di discovery locale. L'host attaccante esegue richieste ARP broadcast ("Who has 192.168.200.150?") per risolvere l'indirizzo fisico (MAC Address) della vittima, preludio necessario a qualsiasi comunicazione IP diretta.



No.	Time	Source	Destination	Protocol	Length	Info
8	28.761629461	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230699	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

Figura 2: Richieste ARP broadcast.

## 2.4 Attacco alle "Top Ports" (Initial Burst)

Immediatamente dopo aver ottenuto il MAC Address della vittima (pacchetto 11), l'attaccante lancia una raffica simultanea di richieste [SYN] verso le porte TCP più comuni ("Top Ports"), visibile dal pacchetto 12 al 18. Questa fase è mirata a identificare rapidamente i servizi standard prima di procedere con una scansione completa.

L'analisi dei pacchetti di risposta (dal 19 al 41) permette di delineare immediatamente il profilo di sicurezza della vittima:

- **Servizi Aperti (Open):** La vittima risponde [SYN, ACK] sulle porte **21 (FTP)**, **23 (Telnet)**, **80 (HTTP)**, **111 (RPC)** e **22 (SSH)**.
- **Servizi Chiusi (Closed):** La vittima invia un [RST, ACK] per le porte cifrate o più moderne come **443 (HTTPS)** e **993 (IMAPS)**.

1. **Riga 12:** Attaccante invia SYN.
2. **Riga 19:** Vittima risponde SYN, ACK.
3. **Riga 24:** Attaccante invia ACK (Connessione stabilita).
4. **Riga 33:** Attaccante chiude con RST, ACK.

12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304	-	23	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535437	Tsecr=0	WS=128	
13	36.774218110	192.168.200.100	192.168.200.150	TCP	74	50120	-	111	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535437	Tsecr=0	WS=128	
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878	-	443	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535437	Tsecr=0	WS=128	
15	36.774356395	192.168.200.100	192.168.200.150	TCP	74	58636	-	554	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535438	Tsecr=0	WS=128	
16	36.774485627	192.168.200.100	192.168.200.150	TCP	74	52358	-	135	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535438	Tsecr=0	WS=128	
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138	-	993	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535438	Tsecr=0	WS=128	
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182	-	21	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535438	Tsecr=0	WS=128	
19	36.774685565	192.168.200.100	192.168.200.150	TCP	74	23	-	41304	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	Tsval=4294952466	Tsecr=810535437	WS=64
20	36.774685652	192.168.200.100	192.168.200.150	TCP	74	111	-	56120	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	Tsval=4294952466	Tsecr=810535437	WS=64
21	36.774685690	192.168.200.100	192.168.200.150	TCP	68	443	-	53978	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
22	36.774685737	192.168.200.100	192.168.200.150	TCP	68	554	-	58636	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
23	36.774685776	192.168.200.100	192.168.200.150	TCP	68	135	-	52358	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
24	36.774706464	192.168.200.100	192.168.200.150	TCP	68	41304	-	23	[ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535438	Tsecr=4294952466			
25	36.774711072	192.168.200.100	192.168.200.150	TCP	68	56120	-	111	[ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535438	Tsecr=4294952466			
26	36.775141164	192.168.200.100	192.168.200.150	TCP	68	893	-	46138	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
27	36.775141273	192.168.200.100	192.168.200.150	TCP	74	21	-	41182	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	Tsval=4294952466	Tsecr=810535438	WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182	-	21	[ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535438	Tsecr=4294952466			
29	36.775337886	192.168.200.100	192.168.200.150	TCP	74	59174	-	113	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535438	Tsecr=0	WS=128	
30	36.775386684	192.168.200.100	192.168.200.150	TCP	74	55656	-	22	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535439	Tsecr=0	WS=128	
31	36.775524264	192.168.200.100	192.168.200.150	TCP	74	53062	-	89	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535439	Tsecr=0	WS=128	
32	36.775589806	192.168.200.100	192.168.200.150	TCP	68	113	-	59174	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304	-	23	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535439	Tsecr=4294952466			
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120	-	111	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535439	Tsecr=4294952466			
35	36.775929330	192.168.200.100	192.168.200.150	TCP	74	22	-	53962	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	Tsval=810535439	Tsecr=4294952466	WS=64
36	36.775979084	192.168.200.100	192.168.200.150	TCP	74	88	-	53062	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	Tsval=810535439	Tsecr=4294952466	WS=64
37	36.775983786	192.168.200.100	192.168.200.150	TCP	66	55656	-	22	[ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535439	Tsecr=4294952466			
38	36.775913232	192.168.200.100	192.168.200.150	TCP	66	53062	-	89	[ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535439	Tsecr=4294952466			
39	36.775961064	192.168.200.100	192.168.200.150	TCP	66	41182	-	21	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535439	Tsecr=4294952466			
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656	-	22	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535439	Tsecr=4294952466			
41	36.776005653	192.168.200.100	192.168.200.150	TCP	66	53062	-	89	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535439	Tsecr=4294952466			

Figura 3: Raffica iniziale sulle porte principali: evidenza delle porte aperte (Telnet, FTP, HTTP) e chiuse (HTTPS).

## 2.5 Enumerazione Infrastruttura e Mail (Second Wave)

Proseguendo la scansione (dal pacchetto 42 in poi), l'attaccante sposta il focus dai servizi di accesso remoto ai servizi di infrastruttura e condivisione file. Questa fase evidenzia una chiara distinzione tra i protocolli supportati dalla macchina vittima.

L'analisi del traffico mostra:

- **File Sharing (Critico):** Vengono rilevate aperte le porte **139 (NetBIOS-SSN)** e **445 (Microsoft-DS)**. La presenza della porta 445 aperta su un sistema Linux/Unix (come indicato dal banner iniziale) suggerisce la presenza del servizio **Samba**, un vettore di attacco frequente per vulnerabilità di tipo RCE (es. SambaCry).
- **Servizi Mail:** È presente una configurazione parziale. La porta **25 (SMTP)** risulta aperta (pacchetto 62), mentre i protocolli di ricezione posta (**POP3 porta 110**, **IMAP porta 143**) e le varianti sicure (**995**, **587**) vengono rifiutati con un RST dalla vittima.
- **DNS:** Viene rilevata aperta anche la porta **53 (Domain Name System)**.

**Evidenza Tecnica:** Le righe 66-68 dello screenshot mostrano nuovamente l'invio dei pacchetti **ACK** da parte dell'attaccante verso le porte 445, 139, 25 e 53. Questo conferma che anche per i servizi infrastrutturali è stata utilizzata una connessione TCP completa, lasciando tracce evidenti nei log del servizio Samba e del Mail Transfer Agent.

39	36	77561904	192.168.200.100	192.168.200.150	TCP	66 53962 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36	77561904	192.168.200.100	192.168.200.150	TCP	66 41102 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36	77561904	192.168.200.100	192.168.200.150	TCP	66 55650 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36	77605853	192.168.200.100	192.168.200.150	TCP	66 53962 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36	776179338	192.168.200.100	192.168.200.150	TCP	74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
43	36	776233880	192.168.200.100	192.168.200.150	TCP	74 54220 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
44	36	776330610	192.168.200.100	192.168.200.150	TCP	74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36	776385564	192.168.200.100	192.168.200.150	TCP	74 33842 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36	776402580	192.168.200.100	192.168.200.150	TCP	74 45814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47	36	776451924	192.168.200.100	192.168.200.150	TCP	66 510 - 36084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36	776451357	192.168.200.100	192.168.200.150	TCP	66 995 - 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36	776478201	192.168.200.100	192.168.200.150	TCP	74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36	776496366	192.168.200.100	192.168.200.150	TCP	74 32606 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51	36	776512221	192.168.200.100	192.168.200.150	TCP	74 60632 - 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52	36	776568666	192.168.200.100	192.168.200.150	TCP	74 49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53	36	776571271	192.168.200.100	192.168.200.150	TCP	74 37282 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54	36	776720715	192.168.200.100	192.168.200.150	TCP	74 54898 - 560 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
55	36	776813123	192.168.200.100	192.168.200.150	TCP	66 587 - 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36	776843423	192.168.200.100	192.168.200.150	TCP	74 51534 - 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
57	36	776904820	192.168.200.100	192.168.200.150	TCP	74 445 - 33942 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
58	36	77694922	192.168.200.100	192.168.200.150	TCP	66 256 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36	776984961	192.168.200.100	192.168.200.150	TCP	74 139 - 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
60	36	776985804	192.168.200.100	192.168.200.150	TCP	66 143 - 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36	776985943	192.168.200.100	192.168.200.150	TCP	74 25 - 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
62	36	776985982	192.168.200.100	192.168.200.150	TCP	66 110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36	776985123	192.168.200.100	192.168.200.150	TCP	74 53 - 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
64	36	776985162	192.168.200.100	192.168.200.150	TCP	66 510 - 36084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36	776917772	192.168.200.100	192.168.200.150	TCP	66 33942 - 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36	776941820	192.168.200.100	192.168.200.150	TCP	66 46990 - 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67	36	776962320	192.168.200.100	192.168.200.150	TCP	66 60632 - 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36	776983870	192.168.200.100	192.168.200.150	TCP	66 37282 - 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69	36	777118481	192.168.200.100	192.168.200.150	TCP	66 487 - 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36	777143614	192.168.200.100	192.168.200.150	TCP	74 56990 - 787 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
71	36	777186921	192.168.200.100	192.168.200.150	TCP	74 35638 - 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
72	36	777392991	192.168.200.100	192.168.200.150	TCP	74 34120 - 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
73	36	77737934	192.168.200.100	192.168.200.150	TCP	74 49780 - 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
74	36	777438632	192.168.200.100	192.168.200.150	TCP	66 787 - 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36	777438741	192.168.200.100	192.168.200.150	TCP	66 436 - 36084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36	777473818	192.168.200.100	192.168.200.150	TCP	74 36138 - 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
77	36	777522494	192.168.200.100	192.168.200.150	TCP	74 52428 - 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
78	36	777623093	192.168.200.100	192.168.200.150	TCP	66 60 - 31620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36	777623149	192.168.200.100	192.168.200.150	TCP	66 78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36	777645827	192.168.200.100	192.168.200.150	TCP	74 41874 - 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
81	36	777688898	192.168.200.100	192.168.200.150	TCP	74 51568 - 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
82	36	777650350	192.168.200.100	192.168.200.150	TCP	66 510 - 31680 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36	777758696	192.168.200.100	192.168.200.150	TCP	66 962 - 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36	777871245	192.168.200.100	192.168.200.150	TCP	66 784 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36	777871293	192.168.200.100	192.168.200.150	TCP	66 435 - 51560 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36	777893298	192.168.200.100	192.168.200.150	TCP	66 33942 - 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36	777912717	192.168.200.100	192.168.200.150	TCP	66 46990 - 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36	777986759	192.168.200.100	192.168.200.150	TCP	66 60632 - 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466

Figura 4: Seconda ondata: Rilevamento di Samba (445), NetBIOS (139) e SMTP (25).

## 2.6 Chiusura Sessioni e Noise Scanning

Immediatamente dopo aver completato l'handshake TCP sulle porte target (fase precedente), l'analisi del traffico evidenzia la fase di "Teardown" (smantellamento) delle connessioni. Nello screenshot, alle righe 86-89, l'attaccante invia pacchetti **RST, ACK** verso le porte precedentemente confermate aperte:

- Porta 445 (SMB)
- Porta 139 (NetBIOS)
- Porta 25 (SMTP)
- Porta 53 (DNS)

Questa azione conferma la natura automatizzata dell'attacco: il tool apre la connessione solo per verificarne l'esistenza e la chiude immediatamente (circa 10ms dopo l'apertura) per minimizzare l'impiego di risorse, pur lasciando traccia nei log.

## 2.7 Rilevamento Servizi Legacy Critici (Porta 512)

L'analisi approfondita del traffico ha permesso di isolare un evento di sicurezza ad alta criticità che era passato in secondo piano durante la scansione massiva.

Alle righe 164-166, si osserva il rilevamento della porta TCP 512.

- **Contesto:** La porta 512 (tcp/exec) fa parte della suite di comandi "R" (r-commands) di Unix/Linux. È un servizio di esecuzione remota noto per la sua debolezza intrinseca (spesso basata solo sull'autenticazione dell'indirizzo IP tramite file .rhosts, senza richiesta di password).

**Dinamica dell'Handshake (Evidence):** Anche in questo caso, la sequenza dei pacchetti conferma la tecnica *Connect Scan* e l'avvenuto contatto con il servizio:



1. **Packet 164:** La vittima risponde [SYN, ACK] dalla porta 512. Il servizio è attivo e in ascolto.
2. **Packet 165:** L'attaccante invia un [ACK] (evidenziato in bianco/blu nello screen). Questo completa la connessione TCP.
3. **Packet 170:** L'attaccante invia [RST, ACK] per chiudere la connessione.

160	36.781321950	192.168.200.100	192.168.200.150	TCP	74	55360	- 918	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535445	Tsecr=0	WS=128	
161	36.781356928	192.168.200.100	192.168.200.150	TCP	74	45648	- 512	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535445	Tsecr=0	WS=128	
162	36.781420319	192.168.200.100	192.168.200.150	TCP	74	53246	- 354	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535445	Tsecr=0	WS=128	
163	36.781487105	192.168.200.150	192.168.200.100	TCP	60	918	- 55360	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512	- 45648	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	Tsval=4294952466	Tsecr=810535445	WS=64
165	36.781512468	192.168.200.100	192.168.200.150	TCP	60	45648	- 512	[ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535445	Tsecr=4294952466			
166	36.781521174	192.168.200.150	192.168.200.100	TCP	60	354	- 918	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
167	36.781548161	192.168.200.100	192.168.200.150	TCP	74	55186	- 858	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535445	Tsecr=0	WS=128	
168	36.781734418	192.168.200.100	192.168.200.150	TCP	74	35806	- 663	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535445	Tsecr=0	WS=128	
169	36.781815101	192.168.200.100	192.168.200.150	TCP	60	358	- 35186	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
170	36.781898537	192.168.200.100	192.168.200.150	TCP	60	45648	- 512	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535445	Tsecr=4294952466			
171	36.782069902	192.168.200.150	192.168.200.100	TCP	60	663	- 35806	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
172	36.782120740	192.168.200.100	192.168.200.150	TCP	74	36210	- 601	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535445	Tsecr=0	WS=128	

Figura 5: Discovery della porta critica 512 (exec). Il pacchetto 165 (ACK) conferma l'avvenuta connessione.

## 2.8 Conferma Vulnerabilità R-Services (Porta 514)

Pochi millisecondi dopo la scoperta della porta 512, l'analisi del traffico evidenzia l'apertura di un ulteriore servizio critico correlato.

Alla riga **267**, la vittima risponde positivamente a una richiesta di connessione sulla porta TCP **514**.

- **Identificazione Servizio:** La porta 514 TCP è standard per il servizio **shell** (cmd). Insieme alla porta 512 (exec) identificata in precedenza, conferma la presenza attiva della suite "R-Services" (rsh, rlogin, rcp).

Anche in questo frangente, il pacchetto n. 268 (ACK) certifica che la connessione è stata pienamente stabilita prima di essere resettata (pacchetto 273), lasciando traccia dell'intrusione nei log del demone inetd/xinetd.

261	36.78903785	192.168.200.100	192.168.200.150	TCP	74	30842	- 773	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535452	Tsecr=0	WS=128	
262	36.788960279	192.168.200.100	192.168.200.150	TCP	74	51396	- 514	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535452	Tsecr=0	WS=128	
263	36.788977629	192.168.200.100	192.168.200.150	TCP	74	56758	- 224	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535452	Tsecr=0	WS=128	
264	36.789107758	192.168.200.100	192.168.200.150	TCP	74	48924	- 183	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535452	Tsecr=0	WS=128	
265	36.788895799	192.168.200.150	192.168.200.100	TCP	60	956	- 48350	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
266	36.788895893	192.168.200.150	192.168.200.100	TCP	60	773	- 30542	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
267	36.788895946	192.168.200.150	192.168.200.100	TCP	74	514	- 51396	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	Tsval=4294952467	Tsecr=810535452	WS=64
268	36.788833247	192.168.200.100	192.168.200.150	TCP	60	51396	- 514	[ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535452	Tsecr=4294952467			
269	36.788954711	192.168.200.150	192.168.200.100	TCP	60	224	- 56758	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
270	36.789010111	192.168.200.150	192.168.200.100	TCP	74	48182	- 361	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535452	Tsecr=0	WS=128	
271	36.789234182	192.168.200.150	192.168.200.100	TCP	60	133	- 48824	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
272	36.789378458	192.168.200.150	192.168.200.100	TCP	60	361	- 48182	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
273	36.789681138	192.168.200.100	192.168.200.150	TCP	60	51396	- 514	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	Tsval=810535453	Tsecr=4294952467			
274	36.789480878	192.168.200.100	192.168.200.150	TCP	74	36846	- 617	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535453	Tsecr=0	WS=128	
275	36.78987028	192.168.200.100	192.168.200.150	TCP	74	34868	- 62	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535453	Tsecr=0	WS=128	
276	36.790932784	192.168.200.150	192.168.200.100	TCP	60	617	- 36846	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
277	36.790962742	192.168.200.150	192.168.200.100	TCP	74	47726	- 8	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535453	Tsecr=0	WS=128	
278	36.790152859	192.168.200.150	192.168.200.100	TCP	60	62	- 34868	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
279	36.790152966	192.168.200.150	192.168.200.100	TCP	60	8	- 47726	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
280	36.790171438	192.168.200.100	192.168.200.150	TCP	74	37560	- 978	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535453	Tsecr=0	WS=128	
281	36.790198641	192.168.200.100	192.168.200.150	TCP	74	58384	- 121	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535453	Tsecr=0	WS=128	
282	36.790247212	192.168.200.100	192.168.200.150	TCP	74	58984	- 186	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535453	Tsecr=0	WS=128	
283	36.790263750	192.168.200.100	192.168.200.150	TCP	74	49848	- 344	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	Tsval=810535454	Tsecr=0	WS=128	
284	36.790407394	192.168.200.150	192.168.200.100	TCP	60	978	- 37560	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					

Figura 6: Rilevamento della porta 514 (shell), confermando l'esposizione della suite R-Services.

## 2.9 Identificazione R-Login (Porta 513)

L'analisi del traffico prosegue rivelando l'ultimo componente della suite di servizi di amministrazione legacy. Si osserva l'handshake completo sulla porta TCP **513**.

- **Packet 988:** L'attaccante invia la richiesta [SYN] verso la porta 513.
- **Packet 994:** La vittima accetta la connessione inviando [SYN, ACK].

- **Packet 997:** L'attaccante finalizza la connessione con [ACK].

986	36.825283652	192.168.200.100	192.168.200.150	TCP	74	38016	- 72	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=0	WS=128	
987	36.825389982	192.168.200.150	192.168.200.100	TCP	69	499	- 43554	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
988	36.825397511	192.168.200.100	192.168.200.150	TCP	74	42048	- 513	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=0	WS=128	
989	36.825414438	192.168.200.150	192.168.200.100	TCP	69	42048	- 39048	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
990	36.825474505	192.168.200.150	192.168.200.100	TCP	69	72	- 38016	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
991	36.825593434	192.168.200.100	192.168.200.150	TCP	74	42110	- 622	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=0	WS=128	
992	36.825645348	192.168.200.100	192.168.200.150	TCP	74	48434	- 457	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=0	WS=128	
993	36.825645296	192.168.200.100	192.168.200.150	TCP	74	48660	- 610	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=0	WS=128	
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513	- 42048	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=810535489	WS=64
995	36.825722761	192.168.200.150	192.168.200.100	TCP	68	622	- 42110	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
996	36.825722768	192.168.200.150	192.168.200.100	TCP	68	457	- 48434	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
997	36.825735068	192.168.200.100	192.168.200.150	TCP	66	42648	- 513	[ACK]	Seq=1	Ack=1	Win=64256	Len=0	TSval=810535489	TSecr=4294952471			
998	36.825835600	192.168.200.150	192.168.200.100	TCP	69	610	- 49660	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
999	36.825892141	192.168.200.100	192.168.200.150	TCP	74	56144	- 680	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=0	WS=128	
1000	36.825994262	192.168.200.100	192.168.200.150	TCP	74	58988	- 267	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=0	WS=128	
1001	36.826117618	192.168.200.100	192.168.200.150	TCP	74	35678	- 82	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=0	WS=128	
1002	36.826171483	192.168.200.100	192.168.200.150	TCP	74	34668	- 951	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535489	TSecr=0	WS=128	
1003	36.826344161	192.168.200.150	192.168.200.100	TCP	68	680	- 56144	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
1004	36.826344247	192.168.200.150	192.168.200.100	TCP	68	267	- 58988	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
1005	36.826344268	192.168.200.150	192.168.200.100	TCP	68	82	- 35678	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
1006	36.826402562	192.168.200.100	192.168.200.150	TCP	74	46854	- 997	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535490	TSecr=0	WS=128	
1007	36.826422755	192.168.200.100	192.168.200.150	TCP	74	48542	- 28	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535490	TSecr=0	WS=128	
1008	36.826516152	192.168.200.150	192.168.200.100	TCP	68	135	- 46854	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
1009	36.826516493	192.168.200.150	192.168.200.100	TCP	68	997	- 46854	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0					
1010	36.826591166	192.168.200.100	192.168.200.150	TCP	74	54134	- 127	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535490	TSecr=0	WS=128	

Figura 7: Rilevamento del servizio login (Porta 513), che completa la triade dei servizi R vulnerabili.

Successivamente, il traffico è caratterizzato da quello che in gergo forense viene definito "Scanning Noise": una serie di tentativi verso porte non standard o casuali (es. 148, 806, 221, 206) che rispondono invariabilmente con **RST, ACK** (rifiuto), indicando che nessun servizio è in ascolto su di esse.

**Estensione dell'Attacco:** È fondamentale notare che questo comportamento persiste per tutta la durata residua del file di cattura. L'attaccante ha continuato sistematicamente a scansionare l'intero range di porte (o un sottoinsieme molto vasto), generando un flusso continuo di risposte [RST, ACK] (visibili come un "muro rosso" in Wireshark) per tutte le restanti porte non attive.

69	36.777118461	192.168.200.150	192.168.200.100	TCP	68	48	- 51534	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74	56990	- 707	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=0	WS=128
71	36.777186081	192.168.200.100	192.168.200.150	TCP	74	35638	- 436	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535440	TSecr=0	WS=128
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	35638	- 436	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49780	- 78	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
74	36.777436032	192.168.200.150	192.168.200.100	TCP	68	67	- 35638	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
75	36.777439741	192.168.200.150	192.168.200.100	TCP	68	436	- 56990	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
76	36.777473013	192.168.200.100	192.168.200.150	TCP	74	51596	- 435	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74	52428	- 902	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
78	36.777623082	192.168.200.150	192.168.200.100	TCP	68	98	- 34120	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
79	36.777623149	192.168.200.150	192.168.200.100	TCP	68	78	- 49780	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
80	36.777645827	192.168.200.100	192.168.200.150	TCP	74	41874	- 764	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51596	- 435	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
82	36.777758636	192.168.200.150	192.168.200.100	TCP	68	590	- 36138	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
83	36.777758696	192.168.200.150	192.168.200.100	TCP	68	902	- 52428	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
84	36.777871245	192.168.200.100	192.168.200.150	TCP	68	764	- 41874	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
85	36.777871293	192.168.200.150	192.168.200.100	TCP	68	435	- 51596	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
86	36.777893298	192.168.200.100	192.168.200.150	TCP	68	38042	- 445	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	TSval=810535441	TSecr=4294952466		
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990	- 139	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	TSval=810535441	TSecr=4294952466		
88	36.777966759	192.168.200.150	192.168.200.100	TCP	68	60632	- 25	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	TSval=810535441	TSecr=4294952466		
89	36.778031265	192.168.200.100	192.168.200.150	TCP	68	37282	- 53	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	TSval=810535441	TSecr=4294952466		
90	36.778173915	192.168.200.150	192.168.200.100	TCP	74	51450	- 148	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
91	36.778208161	192.168.200.100	192.168.200.150	TCP	74	48448	- 896	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535441	TSecr=0	WS=128
92	36.778307830	192.168.200.100	192.168.200.150	TCP	74	54566	- 221	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
93	36.778385946	192.168.200.150	192.168.200.100	TCP	68	148	- 54566	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
94	36.778385948	192.168.200.150	192.168.200.100	TCP	68	896	- 48448	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
95	36.778449494	192.168.200.150	192.168.200.100	TCP	68	221	- 54566	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74	42420	- 1007	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74	34646	- 260	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
98	36.778614055	192.168.200.150	192.168.200.100	TCP	74	54202	- 131	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
99	36.778663864	192.168.200.150	192.168.200.100	TCP	68	1007	- 42420	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
100	36.778721080	192.168.200.150	192.168.200.100	TCP	68	260	- 34646	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
101	36.778758636	192.168.200.100	192.168.200.150	TCP	74	49318	- 392	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74	51276	- 677	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
103	36.778826294	192.168.200.150	192.168.200.100	TCP	68	131	- 54202	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74	39566	- 850	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
105	36.778933827	192.168.200.150	192.168.200.100	TCP	68	392	- 40318	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
106	36.778939427	192.168.200.150	192.168.200.100	TCP	68	677	- 51276	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
107	36.778983153	192.168.200.100	192.168.200.150	TCP	74	47238	- 84	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
108	36.779029210	192.168.200.150	192.168.200.100	TCP	68	850	- 39566	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	30542	- 197	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	68	84	- 47238	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
111	36.779150804	192.168.200.100	192.168.200.150	TCP	74	49318	- 392	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535442	TSecr=0	WS=128
112	36.779258284	192.168.200.150	192.168.200.100	TCP	68	807	- 50542	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43140	- 214	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535443	TSecr=0	WS=128
114	36.779309402	192.168.200.100	192.168.200.150	TCP	74	40886	- 100	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535443	TSecr=0	WS=128
115	36.779345454	192.168.200.150	192.168.200.100	TCP	68	100	- 40886	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
116	36.779378630	192.168.200.100	192.168.200.150	TCP	74	50284	- 138	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535443	TSecr=0	WS=128
117	36.779393072	192.168.200.100	192.168.200.150	TCP	74	51262	- 884	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535443	TSecr=0	WS=128
118	36.779395943	192.168.200.150	192.168.200.100	TCP	68	138	- 50284	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
119	36.779605750	192.168.200.150	192.168.200.100	TCP	68	90	- 40886	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
120	36.779605750	192.168.200.150	192.168.200.100	TCP	68	90	- 40886	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				



### 3 Fase 2: Approfondimento Tecnico (Stealth vs Connect)

Questa sezione dettaglia l'analisi forense che ha permesso di determinare l'esatta tipologia di scansione utilizzata.

#### 3.1 Differenze Teoriche: TCP Connect vs SYN Stealth

Per comprendere l'analisi, è fondamentale distinguere le due modalità principali di scansione TCP:

TCP Connect Scan (-sT)	SYN "Stealth" Scan (-sS)
Esegue il <i>Three-Way Handshake</i> completo.	Esegue un handshake parziale (Half-open).
<b>Flow:</b> SYN → SYN/ACK → ACK → RST	<b>Flow:</b> SYN → SYN/ACK → RST
La connessione viene stabilita a livello Applicativo.	La connessione viene interrotta prima di essere stabilita.
<b>Rilevabilità:</b> Alta. Viene registrata nei log di sistema della vittima.	<b>Rilevabilità:</b> Bassa. Spesso invisibile ai log applicativi standard.

Tabella 1: Confronto tecnico tra le tipologie di scansione.

#### 3.2 Analisi Forense

Analizzando la cattura Wireshark, abbiamo isolato la sequenza di pacchetti relativa alla porta **445 (SMB)**, visibile nello screenshot di prima.

La sequenza osservata è la seguente:

1. **SYN (Attaccante → Vittima):** Richiesta di connessione.
2. **SYN, ACK (Vittima → Attaccante):** Conferma disponibilità della porta.
3. **ACK (Attaccante → Vittima):** *Il punto decisivo.* L'attaccante invia il pacchetto ACK (pacc. n. 66), completando la connessione.
4. **RST, ACK (Attaccante → Vittima):** Solo successivamente (pacc. n. 86) la connessione viene abbattuta.

#### 3.3 Deduzione Investigativa

La presenza del pacchetto **ACK** (terzo step dell'handshake) conferma in modo incontrovertibile che si tratta di una **TCP Connect Scan**. Se fosse stata una scansione Stealth, l'attaccante avrebbe inviato un RST immediatamente dopo aver ricevuto il SYN, ACK, senza mai inviare l'ACK finale.

L'analisi dei pacchetti permette di ricostruire con elevata probabilità le opzioni utilizzate nel tool di scansione (Nmap).

1. **Tecnica (-sT):** La presenza del pacchetto **ACK** inviato dall'attaccante (terzo step dell'handshake) prima del RST conferma l'uso della **TCP Connect Scan**. Se fosse

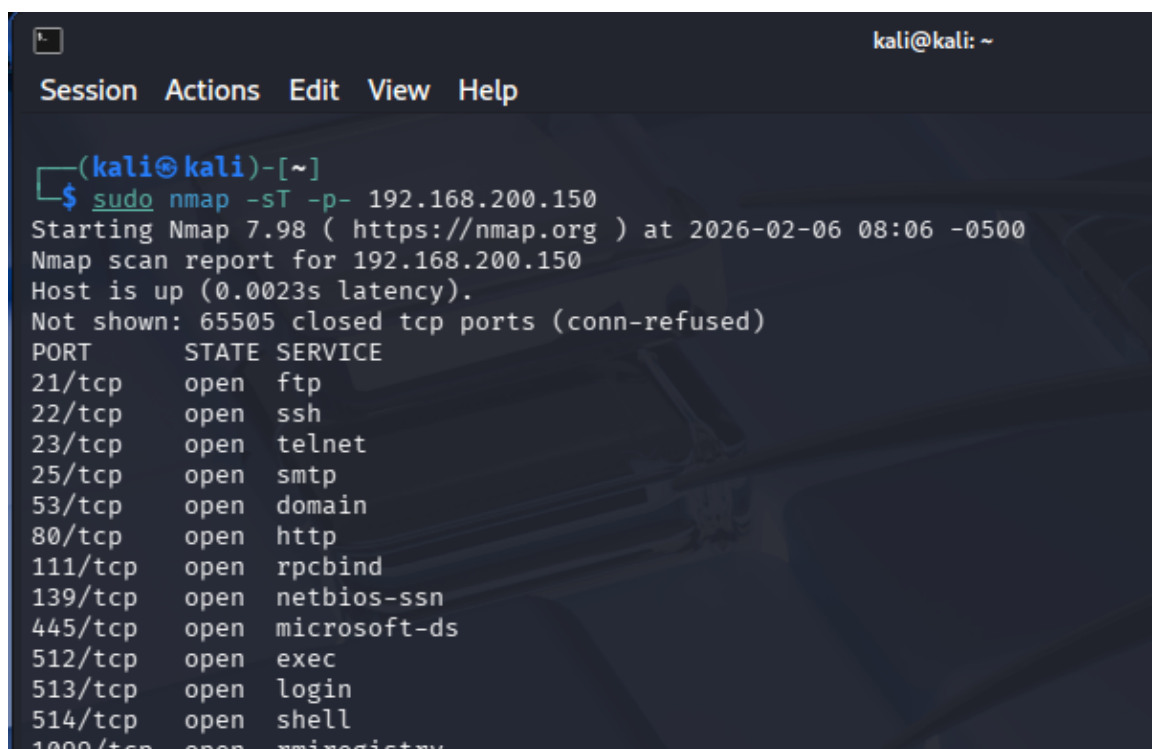
stata una scansione "Stealth" (SYN Scan, default per root), avremmo visto un RST subito dopo il SYN-ACK della vittima.

2. **Estensione (-p-):** L'elevato volume di traffico registrato verso porte non standard e tipicamente chiuse (es. tentativi TCP sulla porta 138, solitamente UDP, o porte randomiche come 118 e 806) indica che l'attaccante non si è limitato alle "Top 1000" porte, ma ha verosimilmente lanciato una scansione sull'intero range di porte (1-65535).
3. **Timing:** La densità temporale dei pacchetti (inviati a intervalli di microsecondi) suggerisce l'uso di un template di timing aggressivo (es. -T4).

**Comando Ipotezzato:** Sulla base delle evidenze, il comando eseguito dall'attaccante è riconducibile alla seguente sintassi:

```
nmap -sT -p- 192.168.200.150
```

**Implicazioni di Sicurezza:** L'utilizzo della flag -sT rende l'attacco estremamente "rumoroso". Poiché ogni connessione verso le porte aperte è stata completata a livello di socket, è altamente probabile che i demoni dei servizi (FTP, SSH, Samba) abbiano registrato l'IP dell'attaccante nei log di sistema della vittima (/var/log/auth.log, /var/log/samba/, ecc.), permettendo una facile attribuzione dell'attacco.



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sT -p- 192.168.200.150  
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-06 08:06 -0500  
Nmap scan report for 192.168.200.150  
Host is up (0.0023s latency).  
Not shown: 65505 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry
```

Figura 9: Comando probabilmente usato dalla Kali vero la Metasploitable.

## 4 Fase 3: Risultati dell'Enumerazione

L'attività di scansione ha avuto pieno successo, permettendo all'attaccante di mappare l'intera superficie di attacco. Di seguito sono elencati i servizi confermati come **OPEN**, suddivisi per tipologia e livello di rischio.

### 4.1 Criticità Massima: Suite "R-Services" (Legacy)

L'analisi ha rilevato l'esposizione della suite completa dei comandi Unix legacy "Berkeley r-commands". Questi servizi sono considerati ad altissimo rischio poiché spesso basano l'autenticazione solo sull'indirizzo IP di provenienza (trust relationship), permettendo accessi root senza password.

- **Porta 512 (TCP exec):** [Rilevata nel pacchetto 165]. Permette l'esecuzione remota di comandi. È il vettore principale per attacchi RCE immediati.
- **Porta 513 (TCP login):** [Rilevata nel pacchetto 994]. Servizio *rlogin*, equivalente non cifrato di Telnet/SSH, ma con meccanismi di trust deboli.
- **Porta 514 (TCP shell):** [Rilevata nel pacchetto 267]. Servizio *rsh* (remote shell). La presenza contemporanea di exec, login e shell conferma che il sistema è obsoleto e non sicuro.

### 4.2 File Sharing e Infrastruttura

Sono stati identificati servizi che espongono il file system o gestiscono risorse di rete, vettori ideali per l'esfiltrazione di dati o attacchi laterali.

- **Porta 445 (SMB) e 139 (NetBIOS):** Servizi per la condivisione file Windows/-Samba. Su sistemi Linux datati, la porta 445 è spesso vulnerabile a exploit critici (es. SambaCry o translatable SID).
- **Porta 21 (FTP):** File Transfer Protocol. Servizio in chiaro, vulnerabile a sniffing delle credenziali e, in alcune versioni (es. vsftpd 2.3.4), contenente backdoor.
- **Porta 111 (RPCbind):** Mappa i servizi RPC su porte di rete. Utile all'attaccante per enumerare ulteriori servizi (come NFS).
- **Porta 25 (SMTP):** Mail Server. Configurato per l'invio, ma con le porte di ricezione (POP3/IMAP) chiuse.
- **Porta 53 (DNS):** Servizio di risoluzione nomi.

### 4.3 Accesso Remoto e Web

- **Porta 23 (Telnet):** Accesso amministrativo remoto obsoleto. Tutto il traffico, incluse user e password, viaggia in chiaro.
- **Porta 80 (HTTP):** Web Server. Potenziale superficie per attacchi web-based (SQL Injection, XSS, CGI vulnerabilities).
- **Porta 22 (SSH):** L'unico servizio di amministrazione cifrato rilevato, sebbene possa essere soggetto ad attacchi Brute Force.

## 5 Conclusioni

L'analisi forense ha confermato che l'host 192.168.200.150 è stato oggetto di una **TCP Connect Scan** massiva proveniente dall'IP 192.168.200.100. Poiché l'attaccante ha completato le connessioni TCP (Three-way handshake), l'attività è stata tracciata nei log di sistema della vittima, rendendo l'attacco facilmente attribuibile.

**Valutazione del Rischio: CRITICA** La scansione ha rivelato una compromissione totale della sicurezza perimetrale. I vettori di attacco più gravi identificati sono:

- **Suite R-Services (Porte 512, 513, 514):** Presenza di servizi legacy che permettono l'accesso *root* senza password.
- **File Sharing (Porta 445):** Rischio elevato di esecuzione codice remoto (es. SambaCry).
- **Protocolli in Chiaro (21, 23):** Credenziali esposte a sniffing.

**Azioni Richieste:** Isolare immediatamente l'host, analizzare i file di log (es. /var/log/auth.log) per confermare eventuali accessi abusivi successivi alla scansione e chiudere le porte non essenziali.